Canadian Journal of Law and Technology

Volume 1 | Number 3 Article 5

8-1-2002

The Patriation of .ca

Gregory R. Hagen

Kim G. von Arx

The Patriation of *.ca*

Gregory R. Hagen† and Kim G. von Arx‡

Introduction

Country code top level domains ("ccTLD"s), such as *.ca*, are distinct from generic top-level domains ("gTLD"s), such as *.com*, in that they are generally conceived to be associated with a specific country.[1] In Canada, the authority to operate the technical functions of the *.ca* domain name registry has been delegated to the Canadian Internet Registration Authority ("CIRA")[2] by a United States non-profit corporation, the Internet Corporation for Assigned Names and Numbers ("ICANN").[3] The authority to make policy regarding the *.ca* has purportedly been delegated to CIRA by the Government of Canada.[4] There is an issue, however, as to whether ICANN's delegation of authority to CIRA to manage the technical functions of the *.ca* reflects a diminished ability of Canada to decide the identity of the *.ca* registry and, by implication, to control the registry's operational policies, thereby diminishing Canada's sovereignty over the *.ca* domain.[5]

While ICANN has been criticized as illegitimate,[6] unfair,[7] anticompetitive[8] and its dispute settlement procedure systematically biased,[9] this paper steps back from those issues and asks whether acknowledging the technical authority of a private foreign entity over the *.ca* domain is consistent with Canada's commitment to political sovereignty. For, as Lessig has pointed out, in cyberspace, code (computer hardware and software) is like law in that code regulates how cyberspace behaves.[10] Applying this observation to the DNS, we argue that the structure of the DNS, which enables the U.S. Department of Commerce ("DoC") to decide who manages the technical aspects of the *.ca*, implies that Canada lacks sovereign control over the *.ca* domain space and related policies and laws.

While the principal of sovereign control over the *.ca* as a Canadian space for e-commerce is important in and of itself, there are also practical consequences that could arise from a lack of control. In short, the hierarchical DNS technology, which ICANN regards as technically necessary, allows the DoC and ICANN to influence critical policies by being able to decide the identity of the *.ca* registry and to tie contractual conditions to the use of a top level domain ("TLD") (i.e., registry operations) and its subdomains. This control enables ICANN and the DoC to create and destroy TLDs and their subdomains, delegate and redelegate domains of any level, and influence areas such as rights to names, trademark law, privacy law, domain name distribution, domain name "taxation", Internet stability and security, authentication policy as well as other areas.[11]

The delegation of power by ICANN to CIRA to operate the *.ca* is the cyberspace analogy to the historical delegation of powers by Parliament in the U.K. to Parliament in Ottawa to enact federal laws governing Canada. Legally speaking, Canada is in a similar position with respect to *.ca* "constitutional law and policy" now as it was with Canadian law prior to the patriation of the Constitution. Analogous to Canada's constitutional powers prior to patriation, Canadian authority over the *.ca* is derived from and depends upon a foreign authority, just as the powers provided for under the Constitution were derived from and depended upon the Westminster Parliament. Consequently, in order for Canada to obtain sovereignty in cyberspace, we claim that policies related to the *.ca* domain should be "patriated" in analogy with the patriation of the Canadian Constitution.

ICANN's Technical Foundation

ICANN was established as an answer to two problems, one technical and one political.[12] The technical problem is how to ensure the stable functioning of Internet services such as web browsing and e-mailing. For example, one should be able to consistently send one's e-mail to its intended destination as defined by the receiver's e-mail address and view the intended web page when a domain name is entered into a browser's location box. The technical answer that has been given is that the DNS must be a hierarchical system, with a single authority, "a unique authoritative root" that, like the baton of an orchestra conductor, tells Internet users how to find the authoritative domain name mappings.[13]

†Replacement Assistant Professor, University of Ottawa, Faculty of Law. A previous version of this paper was submitted in partial fulfillment of the requirements for the LL.M. (concentration in law and technology) at the University of Ottawa.

‡Legal counsel to Canadian Internet Registration Authority (CIRA). The opinions expressed herein are not necessarily those of CIRA.

On this model, whoever controls the root is the orchestra conductor.

The existence of a hierarchical system of domain name servers on the Internet is somewhat surprising when one considers that one of the most fundamental aspects of the Internet is the absence of a locus of control. The original motivation for such a packet switched network was that of redundancy, or the requirement that there should be no single point of failure (or control) under an attack on the network.[14] A related fundamental principle is the idea of "end-to-end reasoning". Reed and Saltzer have explained this concept as the idea that, in a communications system, a function "can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system".[15] Similarly, Isenberg has written about a new philosophy and architecture where "intelligence" is at the edges of the network rather than in the network itself is developing. He writes that "it would be engineered for intelligence at the end-user's device, not in the network. And the network would be engineered simply to 'Deliver the Bits, Stupid,' not for fancy network routing or 'smart' number translation".[16]

In order to further understand the technical solution, it is useful to consider that each computer host on the Internet is assigned a unique Internet protocol ("IP") address which encodes both a network and host identifier.[17] Because IP numbers are difficult for people to remember and lack portability, Internet standards provide for the creation of domain names for computer hosts. These names also allow for easy memorization and host name portability over changing Internet service providers. The assignments of domain names to IP addresses were recorded in a central "root" database administered by a single person. As such registrations increased, however, a hierarchical naming system was created in order to lessen the administrative burden of name assignments. In essence, TLDs were registered by the root authority, and the registration of subdomains of TLDs was delegated to TLD registries.

The legacy root (often called the "A root"), or highest level, of the name space is unnamed. Below the legacy root are TLDs that are divided into classes according to their use as military, educational, government, commercial, territorial, and so on. Currently, there are 257 top level domains. There are a total of three types of TLDs, two of which are relevant here. One is the "gTLD", such as *.com*, *.net*, *.mil*, *.gov*, etc.[18] These TLDs are "generic" in the sense that they are generally viewed as global because they are not associated with any specific territory.[19] The second type of TLD is the "ccTLD", such as *.ca* (Canada), *.de* (Germany), *.uk* (United Kingdom), *.tv* (Tivoli), *.ch* (Switzerland), *.au* (Australia), and *.jp* (Japan), of which there are currently 243. These ccTLDs have been delegated to registries, whose codes are assigned from a table known as ISO-3166-1, which is maintained by the International Organization for Standardization (ISO). Beneath the top level domains are second level domains such as *gc.ca*, third level domains such as *ic.gc.ca*, and so on. Finally there is one infrastructure TLD ("iTLD") called *.arpa*. The iTLD is the Address and Routing Parameter Area domain and is used to perform mappings of domain names to IP addresses.[20]

Many registries, such as CIRA, outsource to registrars the service of recording registrations in their respective registries (while some registries, such as the TV Corporation, record names themselves). In order to initially obtain a second level domain name assignment (or a third level domain name assignment in the case of those registries, e.g., Australia and the United Kingdom, who generally permit only third level domain registrations), a person whether natural or juridical ("registrant") registers an available domain name with the registry via a registrar or the registry directly. The relevant entity then record the registrant's name, contact information, and often at least two IP numbers which point to servers which can resolve the name. Conflicting name mappings are avoided primarily by allocating domain names in the gTLDs and most of the ccTLDS on a first-come, first-served basis.[21] The responsibility for adoption of procedures and policies for the assignment of second level domain names (or third level, in the cases mentioned above) and lower level hierarchies of names is delegated to TLD registries, subject to the policy guidance contained in ICANN policies and any agreements that may exist between the TLD registry and ICANN.

Certain authority relations are coded into the DNS. When a user types in a domain name into a browser, a client-sided resolver usually queries a local Internet Service Provider (ISP) name server to search its corresponding database of resource records for a record of the necessary assignment. Certain kinds of resource records, called "zone files", contain the assignments of domain names to IP addresses for a particular zone, which is a portion of a domain space. By pointing its resolver to the ISP name server, the Internet user implicitly acknowledges the authority of the ISP name server's response. If the ISP cannot provide the relevant assignment because it has not been cached, or the validity of the information has expired, the ISP server usually queries one of the 13 legacy root name servers.[22] Thus, the ISP also implicitly accepts the authority of the root server to which it points. The root name server is associated with a master file called the "root zone file" that lists the name and location of the TLD servers that the root operator considers authoritative.[23]

So long as everyone recognizes the same family of hierarchically organized databases as authoritative, with the legacy root name server at the top, the mappings of domain names to IP address, including those contained in the root zone file, will be unique with respect to that DNS.[24] In essence, on this approach, the uniqueness of name-to-address mappings in the legacy DNS is guaranteed because there is ultimately one unique authoritative

root server managed by ICANN, subject to its ultimate control by the DoC, from which the entire legacy name space is derived.

ICANN's Political Foundation and Its Implications

The second reason for ICANN's existence is political. It is the answer to the query "who should control the legacy root"? Whoever controls the root controls which, and how many, TLDs will be entered into the legacy root *and* who will be the registry for each TLD. ICANN has declared that *it* is the proper entity to manage the unique authoritative root, answering the basic political issue surrounding the current DNS.[25] Thus, despite the underlying end-to-end design philosophy of the Internet, a central point of control is used as a means of coordinating Internet activities and regulating domain names.[26]

Instead of the metaphor of an orchestra, with ICANN as a conductor, Reed describes the tendency to control as a more sinister invasion of trolls setting up shop under our network bridges who must bless any new protocols or applications.[27] Yet, ICANN did not begin its life as such a troll. Due to the early funding of the Internet by U.S. government agencies, the United States government found itself in the, perhaps unwanted, position of exercising control over the legacy root. By the mid-1990s, the growth and increasing commercialization of the Internet led the U.S. government's Green[28] and White Papers[29] to note the emergence of widespread dissatisfaction about the absence of competition in domain name registration. The White Paper called for the government to transfer control of the DNS to a private corporation. Subsequently, a California nonprofit corporation called ICANN was established essentially by Jon Postel, and the government duly recognized ICANN as the private organization which has the support of the Internet community to administer the functions of the legacy root.[30]

The White Paper noted that some commentators expressed concern that the suggested privatization plan in an earlier Green Paper did not go far enough in "globalizing" the administration of the domain name system.[31] Some believed that international organizations should have a role in administering the DNS.[32] Others observed that incorporating the new corporation in the United States would entrench control over the Internet with the U.S. government.[33] The United States government responded to these concerns in the White Paper:

> The U.S. Government believes that the Internet is a global medium and that its technical management should fully reflect the global diversity of Internet users. We recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management.[34]

Canada endorsed the United States' privatization of the DNS on the basis that privatization "divested U.S. government agencies of control of DNS functions and placed control in the hands of a 'private sector' group".[35] Despite Canada's stated interest that the U.S. divest control over the DNS, the United States never did withdraw control over the legacy root server.[36] In fact, the U.S. General Accounting Office questioned whether the U.S. government had the authority to transfer control of the root server to ICANN and has not examined such issues because there are no plans to transfer control over the legacy root. It said:

> The question of whether the Department has the authority to transfer control of the authoritative root server to ICANN is a difficult one to answer. Although control over the authoritative root server is not based on any statute or international agreement, the government has long been instrumental in supporting and developing the Internet and the domain name system. The Department has no specific statutory obligations to manage the domain name system or to control the authoritative root server. It is uncertain whether transferring control would also include transfer of government property to a private entity. Determining whether there is government property may be difficult. To the extent that transition of the management control to a private entity would involve the transfer of government property, it is unclear if the Department has the requisite authority to effect such a transfer. Since the Department states that it has no plans to transfer the root server system, it has not examined these issues. Currently, under the cooperative agreement with Network Solutions, the Department has reserved final policy control over the authoritative root server.[37]

According to the same review of the privatization of the DNS, Counsel for the United States General Accounting Office stated bluntly: "According to the Department, it has no current plans to transfer policy authority for the authoritative root server to ICANN, nor has it developed a scenario or set of circumstances under which such control would be transferred."[38] Nancy Victory, Assistant Secretary of Commerce for Telecommunications and Information commented:

> Regarding the A Root server, the Department of Commerce has no plans to transfer policy control … When the necessary technical capacity is in place, the department may enter into a management agreement or other legal arrangement with ICANN for operation of the A Root server.[39]

More recently, the Energy and Commerce Committee sent a letter to Secretary Donald L. Evans of the DoC reiterating its view that "any assumption of control over that asset [the legacy root] by any outside entity would be contrary to the economic and national security interests of the United States."[40] Recent terrorist attacks on the U.S. have increased its reluctance to divest control. Andy Müller-Maguhn, Europe's ICANN Director, is reported to have said:

> It might be that after the Sept. 11 attacks, the U.S. government is not behaving as if it would give any kind of

> control away. It doesn't look like it at least to me, to be honest, not all. If the United States government never plans to give authority over the root zone files to ICANN … then the issue might be raised … if it's just the simulation of an institution where the real power is the United States government.[41]

ICANN's power, then, is not the power to control the legacy root server, which has been retained by the U.S. government. Instead, ICANN's power rests in its management of DNS functions, which stems from its contract with the United States DoC. The Memorandum of Understanding between ICANN and the United States Government provides as its purpose that "the Parties will jointly design, develop, and test the mechanisms, methods, and procedures that should be in place and the steps necessary to transition management responsibility for DNS functions now performed by, or on behalf of, the U.S. Government to a private-sector not-for-profit entity."[42] Under this Agreement, ICANN's powers do nothing to alter control over the legacy root:

> This [administrative] function, however, does not include authorizing modifications, additions, or deletions to the root zone file or associated information that constitute delegation or re-delegation of top-level domains. The purchase order will not alter root system responsibility defined in amendment 11 of the Cooperative Agreement.[43]

Notwithstanding this reservation of rights, ICANN is on a short leash. The U.S. government can terminate the agreement on 120 days notice to ICANN.[44]

Nevertheless, subject to approval by the U.S. Government, ICANN possesses the power to withdraw the authority of any registry, such as CIRA, to act as the registry of their respective ccTLDs, including the subdomains, and can transfer the ccTLD to other entities or persons without such registry's consent.[45] Indeed, Stuart Lynn, ICANN's president, recently summed up the power that ICANN has over country code domains: "ICANN could, in theory, recommend that a particular ccTLD be redelegated to a cooperating administrator, and if the US Government accepted that recommendation, non-cooperating ccTLD administrators would be replaced".[46]

The most straightforward implication of ICANN's control is its apparent ability (to be discussed in more detail below) to redelegate domain names, contrary to any national legal requirements that a particular entity be assigned such a domain name. For instance, at the highest level, while the Government of Canada may have delegated CIRA as the authoritative *.ca* registry, the U.S. DoC is able to remove the *.ca* from the legacy root server or map the *.ca* to IP addresses of a TLD name server controlled by a different entity. By implication, ICANN is also able to force the redelegation of second level and lower domains, such as *gc.ca* and *ic.gc.ca*. More subtly, ICANN can tie conditions to the use of domain names, including requiring registries, registrars and registrants to conform to ICANN policies. For example, under the Model Legacy Memorandum Agreement between ccTLDs and ICANN, a registry must comply with any policies established through the ICANN policy-development process.[47] Even if such policies were limited to those involving "technical coordination", ICANN has construed the notion of "technical coordination" quite broadly so as to include intellectual property, privacy and competition policy.[48] This would provide ICANN with a means to control registry and registrar operations and policies, such as registrant and registrar agreements.

One might argue, at this point, that it is ludicrous to believe that the U.S. would threaten the stability of the Internet in order to redelegate a single second level domain, such as *gc.ca*, let alone a TLD, such as *.ca*. Moreover, it could be argued that, if a power struggle commenced (because, for example, CIRA refused to sign the model Sponsorship Agreement) and the U.S. subsequently did remove *.ca* from the root zone file, services using *.ca* domains would not come to a sudden halt. Firstly, ISP name servers cache the most commonly used *.ca* domains and therefore, the mappings to appropriate IP addresses would not end until the validity of mapping data in those zone files expired. Secondly, either CIRA itself or major ISPs would begin to offer root server services, replacing those offered by ICANN.

The difficulty with this idea is that, even if such root server services could be provided, it requires ISPs worldwide to recognize the new root. If ICANN redelegated *.ca* to another organization whose operations, for the sake of argument, were in the U.S., then the attempt by CIRA or an ISP to supply *.ca* services would potentially conflict with those services supplied by the redelegated *.ca* registry. In such a situation, it is likely that most ISPs would rely upon the legacy server system rather than CIRA's *.ca*. The moral is that, while CIRA *.ca* services may continue to work after ICANN's removal or redelegation of *.ca*, the maintenance of Canadian control over the *.ca* would require modifications to the DNS protocols and architecture so that other ccTLDs recognized CIRA's authority over *.ca*. This paper simply advocates making the requisite changes to the DNS architecture sooner rather than later.

A second example of ICANN's power over *.ca* is its effects on the privacy rights of registrants. ICANN's Model Sponsorship Agreement — as well as the subsisting agreements with Australia and Japan ccTLD registries — provides that "[t]he Sponsoring Organization shall ensure that the zone file and accurate and up-to-date registration data for the Delegated ccTLD is continuously available to ICANN, in a manner which ICANN may from time to time reasonably specify, for purposes of verifying and ensuring the operational stability of the delegated ccTLD only".[49] There is a requirement, then, that the technology of the TLD database must allow ICANN continuous access to registration data. This obligation may contradict the Canadian *Personal Information and Protection of Electronic Documents Act* requirement that disclosure of information to a third

party must be with the consent of the subject of the personal information in those cases where the registrant objects to its disclosure to ICANN.[50]

The simplest, but probably most significant implication of ICANN's control over *.ca*, however, is that the U.S. will be able to apply what is essentially a foreign domain name "tax" to *.ca* domain name registrants. This results from the fact that the Model Sponsorship Agreement requires CIRA to contribute to ICANN's cost of operation in accordance with the formula devised by ICANN. To give an idea of the potential magnitude of the tax, consider that the Sponsorship Agreement caps the fixed annual portion of the CIRA contribution at US$5000 and caps the variable portion of the total annual fee at US$5,500,000 for the fiscal year ending June 30, 2002. And while the Agreement provides that the cap shall increase by 15% each fiscal year thereafter, ICANN may increase the tax by a greater amount without CIRA's consent.[51] CIRA and its registrants may begin to wonder if ICANN's root server services are worth the price.

A Friendly Redelegation: The Case of the Mysterious Double Delegation to CIRA

CIRA is a not-for-profit Canadian corporation that is responsible for operating the *.ca* ccTLD for all Canadians in an efficient and professional manner.[52] The Canadian government, in its communications with CIRA and ICANN, has attempted to instantiate the U.S. distinction between technical coordination and policy authority. This distinction, outlined in the U.S. government's White Paper, holds that "national governments now have, and will continue to have, authority to manage or establish policies for their own ccTLDs", but that "the U.S. continues to believe, as do most commentors, that neither national governments acting as sovereigns nor intergovernmental organizations acting as representatives of governments should participate in management of Internet names and addresses".[53]

As regards technical coordination, the Canadian government took the position that it " … supports the basic principles of introducing competition but minimizing government involvement in the actual running of the DNS".[54] While CIRA is responsible for operating the *.ca*, "[t]he Government of Canada … has recognized ICANN's primary responsibility for establishing, disseminating, and overseeing implementation of the technical standards and practices that relate to the operation of the global DNS".[55]

In terms of policy, the Canadian government's position is presently that "the *.ca* domain space is a key public resource, helping to promote the development of electronic commerce in Canada and important to our country's future social and economic development".[56] CIRA takes a similar position.[57] More generally the Government of Canada has confirmed that it has "overall policy responsibility for the Information Highway".[58] Under the ICANN Government Advisory Committee Operating Rules, the "ultimate public policy authority over the relevant ccTLD rests with the relevant government or public authority".[59] As a result of its overall policy authority, the Canadian government explicitly set out specific principles which it expected CIRA to implement in its policies.[60]

Originally, Jon Postel of Internet Assigned Numbers Authority (IANA)[61] delegated the management of the top level Canadian *.ca* domain to John Demco of the University of British Columbia (UBC).[62] There was no formal delegation of policy authority by the Canadian government to Demco. Prior to the transfer of authority to CIRA, John Demco and his group had managed the *.ca* ccTLD on a voluntary basis with the help of the *.ca* committee, at no charge to users.[63] At an Internet conference in June 1997 in Halifax, however, concerns were expressed about the delay in obtaining *.ca* domains which generated widespread dissatisfaction within the Canadian Internet community where, under rules of delegation, timely responses to registration requests are a priority.[64] Following the 1997 meeting, then, it was generally agreed that the Canadian Domain Name Consultative Committee ("CDNCC") should be created to address the transition from the current management of the *.ca* domain to a commercial operation.[65]

The CDNCC report proposed that a non-profit entity be created much as had been proposed by the earlier Green Paper in the United States. As a result, CIRA was incorporated as a non-profit corporation on December 3, 1998. Industry Canada noted that because its basic goal was to privatize operation of the DNS, the role of government in the transition process to a new governing body is "naturally fairly limited".[66] The Government of Canada has interpreted its "fairly limited" role as that of delegating its inherent policy authority over the *.ca* domain to this private corporation, CIRA. Thus, on October 10, 2000, the Canadian government wrote ICANN, stating that it "recognizes CIRA as the administrator of the .CA. domain",[67] and "formally designate[s] CIRA as the Government of Canada's designee to be the .ca delegee".[68] In the same document, it also set out certain general principles by which it expected CIRA to abide.

IANA redelegated the technical authority over the *.ca* domain to CIRA on December 3, 1998, and also outlined the technical functions that CIRA would be expected to perform in accordance with ICANN policies.[69] The redelegation went rather smoothly, mainly because all concerned parties agreed upon the redelegation of *.ca* to CIRA.[70] The basis of the power of delegation is provided for in RFC 1591[71] written by Jon Postel in 1994. ICANN subsequently adopted policy ICP-1[72] which modifies RFC 1591. The modifications have the

effect of giving more power to ICANN than it had under RFC 1591. However, these additional powers did not need to be implemented given the friendly transfer of power to CIRA.[73]

Although CIRA was founded upon the idea that policy authority and technical authority over the *.ca* converged in it, it has been argued here that the need for the delegation of technical authority to CIRA — which makes a subordinate name server authoritative over TLD subdomains — ultimately reserves a power in the delegator to influence policies with respect to the *.ca* TLD. In the delegation process, the necessity of the technical authority to enable public policy authority is evident where, in its letter to ICANN, the Canadian government requested that ICANN effect the necessary changes to the Internet's "legacy" root server to enable CIRA to operate the *.ca* in accordance with Government of Canada policies.[74] At present, then, Canada is not sovereign over the *.ca*.

Hostile Redelegation

Two recent hostile redelegations vividly emphasize DoC's and ICANN's ability to redelegate ccTLDs over objections from the current ccTLD. In each case, the national government wanted the redelegation to occur while the existing TLD registry did not. The redelegations demonstrate that physical control over the operation of the ccTLDs lies with ICANN and the DoC. As has been pointed out, control over the architecture of the Internet generally, and the DNS specifically, enables one to control law and policy relating to DNS functions. The power to redelegate domains provides ICANN and the DoC with the ability to influence or control the operational policies of registrars and registries and to tie conditions to the use of domain names which, in essence, constitutes domain name law and policy.

The first example concerns ICANN's hostile redelegation of the Australian Internet domain name space, namely all the domain names ending in *.au*.[75] ICANN used this opportunity to force the new *.au* registry to sign a Sponsorship Agreement with ICANN by making the redelegation contingent upon its execution. In that case, ICANN redelegated the top level domain as well as second level domains, such as *org.au*,[76] over the objections of both the current *.au* registry[77] and the *.org.au* registry, without any finding of misconduct and without a public comment process.[78]

Redelegation consists of two stages: first, there is the revocation of authority from an existing registry. Under ICANN rules, ICANN "must receive communications from both the old organization and the new organization that assure the IANA [i.e. ICANN] that the transfer is mutually agreed".[79] Ignoring its own policy, ICANN justified withdrawing Robert Elz as the registry manager based on the idea that "there is widespread — nearly universal — support for moving the delegation of the .au ccTLD to an organization permitting broad participation of the Australian Internet community in the development of policy for the .au ccTLD".[80]

The second stage is the delegation of authority to a new registry. In this matter, ICANN took the Australian government's wishes to redelegate to the new auDA registry as decisive, citing the policy of ICP-1 that the "[t]he desires of the government of a country with regard to delegation of a ccTLD are taken very seriously. The IANA [i.e. now operated by ICANN] will make them a major consideration in any TLD delegation/transfer discussions".[81] ICANN also referred to the fact that the GAC Principles for Delegation and Administration of ccTLDs were satisfied as a reason for delegating to the new .au registry. Under the GAC principles, the government is authoritative over its own ccTLD policy and decides the identity of the ccTLD registry.[82]

Perhaps the most interesting example of the use of the U.S. power to redelegate (without any regard to other ccTLDs)[83] is the apparently hostile redelegation of the *.us* domain to Neustar. In this case, ICANN did not give as its rationale the need to transfer the *.us* to an accountable organization, since it had presumably already done so when it delegated the *.us* registry functions to Verisign's predecessor, Network Solutions. Like Verisign, Neustar is a for-profit corporation owned by its shareholders and not a non-profit corporation accountable to its members. Although the U.S. government did not enter into a Sponsorship Agreement with Neustar, to whom *.us* was redelegated, it does show that the U.S. DoC is prepared to redelegate despite the ccTLD having been previously delegated to a well-run corporate registry, such as Verisign. Perhaps the DoC felt that there was no need to enter into a Sponsorship Agreement with Neustar because the DoC believed that it could control Neustar, a U.S. company, more easily than a foreign corporation.

In fact, the U.S. government accomplished the redelegation to Neustar unilaterally and without ICANN's approval. This transfer was completed "before the completion of the normal IANA requirements",[84] which under ICP-1 and RFC 1591 require a formal written agreement. It was apparently done without the approval of the then existing *.us* registry and without the written agreement required by GAC. While the earlier hostile redelegation of *.au* was done with ICANN's full approval, the redelegation of *.us* was not. The official, and somewhat obscure, explanation from the U.S. government was that "because of complexities of U.S. procurement laws, it was not able to extend the existing arrangements with VeriSign nor complete the necessary three-way set of communications among itself, ICANN, and NeuStar".[85]

ICANN's explanation for its redelegation of the root was essentially an admission that it does not have any power to stop the U.S. government from changing data in the A Root, so it must make the change in the legal

delegee of authority to concur with the change of information in the root. Indeed, ICANN admits that if it had not accepted the request from the U.S. it would have "created a situation where the event would have occurred regardless but there would be inconsistent data in the IANA database".[86] Given ICANN's primary mission focus on technical stability, ICANN had to comply with the DoC's wishes.

Sovereign Claims and Property Law

While Internet architects are primarily interested in technical stability — the uniqueness of name mappings to IP addresses — national governments have become increasingly interested in national sovereignty over ccTLDs.[87] National sovereignty over ccTLDs would ensure that the national government could control country code domain name mappings and related policies above and beyond the uniqueness requirement. Such control would ensure that the identity of the registry and the users of domain names and related concerns were subject to national law rather than foreign control.

National governments, through the Government Advisory Committee of ICANN, have attempted to found their claims to sovereignty over their respective ccTLDs by claiming that ccTLDs are "public resources".[88] Moreover, claims that domains are property have been made at both the TLD level and lower levels. By subjecting domain names to property rules, one can ensure the persistence of TLD and other domain name assignments in the sense that once validly owned, domains cannot be transferred to a third party without consent, expiration of ownership, or termination under applicable law. Property rules are to be contrasted with liability rules grounded in contract which compensate invalid transfers of domain names monetarily.[89]

Network Solutions (the predecessor in interest to the existing *.com* registry, Verisign) has suggested that it possesses trademark rights in the *.com* TLD as well as the *.com* brand and rights to the database of registrant information.[90] While some domain names are trademarks and, therefore, the risk of a company losing its trademarked domain name under a hostile redelegation is minimized, such protection only applies to trademarked domain names and will not apply where a new registrant of the trademarked domain is not making an infringing use of it. Thus, one would have to look to a general property right in domain names to ensure stability over hostile redelegations rather than trademark law.

Secondly, the claim that domain names are public property cannot be sustained given the nature of ownership of the Internet. The legacy root server is owned by the United States government and arguably its contents are, too. TLD name servers are owned by the TLD registries, and ISP name servers are owned by the respective ISPs. Thus, if domains are property, they are likely to be private property based upon the private ownership of the physical objects underlying the domain names.

Thirdly, there is the difficulty that it is not widely accepted that domain names *per se* are property.[91] TLDs are delegated on the basis of an arrangement, sometimes reduced to writing, with ICANN. Second (and sometimes third) level domain names are then obtained by entering into a contract with a domain name registrar and therefore are, *prima facie*, contractual in nature. The contract to provide naming services is generally non-assignable, indicating that it does not have the transferability of property. This point of view has been affirmed in the U.S. case *Zurakov v. Registrar.com*, in which the court found on summary judgment that:

> The question of whether a domain name is a "property right" has not been considered by the courts of this state. Accordingly, this court looks to courts in other jurisdictions that have opined on this issue. In *Network Solutions, Inc. v. Umbro International Inc.*, 529 S.E.2d 80 (2000) the Supreme Court of Virginia stated that, "a domain name registrant acquires the contractual right to use a unique domain name for a specified period of time". The Network Court relied on *Dorer v. Arel*, 60 F.Supp.2d 558, 561 (E.D. Va. 1999). In that case, the court stated that "[a] domain name that is not a trademark arguably entails only contract, not property rights. Thus, a domain name registration is the product of a contract for services between the registrar and registrant".[92]

The case of *Lockheed Martin Corp. v. Network Solutions, Inc.* is much to the same effect.[93]

However, contrary authority does exist. In *Kremen v. Cohen*, for example, the Court determined that although the domain name "*sex.com*" was not tangible property under United States law, it was nonetheless a form of intangible property.[94] There have also been claims brought *in rem* — that is, a claim against the property itself — against a domain name under the *United States Anticybersquatting Consumer Protection Act*.[95] As this appears inconsistent with the decisions that hold that a domain name is not property, it seems to indicate Congress's intention to affirm that domain names are in some instances indeed property, at least for procedural and execution purposes.[96] The constitutionality of this legislation has been upheld.[97] Nevertheless, the scope of the property right extends only to domain names that are trademarks, and thus cannot support the claim that domain names *per se* are the subject of property rights.[98]

In Canada, there does not seem to be decisive authority regarding the status of domain names as property. In *Easthaven, Ltd. v. Nutrisystem.com Inc.*,[99] Nordheimer J. found that domain names do not seem to be property, but that even if they were, since they exist only intangibly in cyberspace, they are not located in Ontario, Canada.[100] The Court therefore dismissed the plaintiff's claim that "*sweetsuccess.com*" was property located in Canada. Nordheimer J. states his views in remarkably ambiguous language:

> It does seem to me to be difficult to characterize a domain name as property. When I say property, I refer to either real or personal property. I appreciate that a domain name, like a copyright or a trade-mark, could be properly characterized as intangible property. It does seem to me to be difficult to characterize a domain name as property.[101]

While the status of domain names is unsettled, sovereign control over domain name mappings cannot be definitively supported by property law. The central difficulty is that, even if there were domestic property rights in domain names, there would still be the problem that a foreign government has the power to modify information contained in the legacy root server, which will regulate behaviour, regardless of any property laws that may apply to domains. For example, if the Canadian government enacted a law declaring that it is the owner of the *.ca* TLD, it would have little practical effect. Foreign control over the root implies that the foreign authority can decide who is assigned the *.ca*, can redelegate the domain and its subdomains against the wishes of the registry, and can attach conditions and obligations to the use of such domains.

A Parallel with Constitutional Law

John Perry Barlow famously declared the independence of cyberspace from territorial sovereigns.[102] The basic claim to independence results from the fact that because, given current technology, the Internet does not yet have naturally occurring borders, the network itself defines a new distinct jurisdiction that can create its own laws and legal institutions.[103] If cyberspace is independent of territorial sovereigns, then ICANN's declaration that it is the unique authoritative root for the domain name space in cyberspace is tantamount to declaring itself sovereign over the entire namespace, including the *.ca* domain.

As David Post observed in 1998, the formation of ICANN was a "constitutional moment" and "an exercise in a kind of constitution-making, the creation of a global governing entity with ultimate authority over this most extraordinary (and most valuable) global resource".[104] As Post has pointed out further, the liberal doctrine of the sovereign state does not necessarily posit ultimate sovereignty in the territorial state, but is derived ultimately from individual people who are sovereign within that territory.[105] Therefore, ICANN might be considered the sovereign authority over the domain space of gTLDs and ccTLDs as a result of the collective consent of geographically dispersed Internet users.[106]

However, ICANN itself is ultimately controlled by the United States Government, both in terms of the technical functions that ICANN performs and the U.S. Government reservation of authority over the information contained in the root zone file. Therefore, any use of the ICANN domain space is ultimately subject to control by the U.S. government. It turns out that, insofar as cyberspace is restricted to ICANN domain space, cyberspace did not gain independence from territorial governments, but rather reflects the ability of a foreign government to extend an extraterritorial reach into cyberspace and beyond. From this point of view, ICANN's delegation of authority to TLD registries is analogous to the delegation of lawmaking power to colonies of an imperial government.

The question that arises is whether *.ca* is a cyberspace colony of the U.S., depriving Canada of sovereign authority over its name space and its related policies. As mentioned, these policies and laws not only include "constitutional" policies, such as CIRA bylaws, registrar and registrant agreements and dispute settlement policies, but laws and policies that are affected by the DNS, such as authentication, privacy, trademark, and other laws. If it is, can Canada gain sovereignty over the *.ca* by patriating it and its related policies as it did in the case of the Canadian Constitution?

The term "patriation" is of uniquely Canadian origin, derived from the verb "repatriate" which means "to restore to one's own country". As Hogg points out, since the *British North America Act 1867* was not a Canadian Act, it could not be "restored" to Canada. Patriation, therefore, conveys the idea of a Constitution becoming a Canadian instrument.[107] What, then, is the nature of the patriation of the Canadian Constitution? The answer of autochthony, which requires that a constitution be indigenous and derive its authority solely from events occuring within Canada, is not, therefore, the basis of the patriation.[108] The legal force of the *Canada Act 1982* and the *Constitution Act 1982*, like other U.K. statutes which extend to Canada, depends upon the power that the United Kingdom Parliament has over Canada. These instruments depend upon an external rather than a local root.[109]

A second possible explanation of the nature of patriation posits that its force derives from the legal termination of the imperial authority of the United Kingdom. Pursuant to the *Canada Act 1982*, s. 2, "[n]o Act of the Parliament of the United Kingdom passed after the *Constitution Act 1982* comes into force shall extend to Canada as part of its law."[110] This discontinuity in the United Kingdom's ability to legislate over Canada might have been thought a sufficient discontinuity to make the Queen in right of Canada (but not in right of the United Kingdom[111]) Canada's ultimate source of legal authority. However, under the traditional view of parliamentary sovereignty, this cannot be correct since, under that view, the United Kingdom could at any time repeal s. 2 of the *Canada Act 1982*. Accordingly, the current Parliament could not bind future Parliaments by its present enactments and, therefore, could not be bound to refrain from enacting laws for Canada. In fact, some scholars believe that there is a paradox of self-reference involved in thinking that any *Grundnorm* (basic norm), such as a law regarding the amendment of a constitution, could itself be amended, since, by hypoth-

esis, the basic norm would then no longer exist to justify the new rule regarding amendment.[112]

Prior to the *Constitution Act 1982*, the major constitutional document of Canada was the *British North America Act, 1867*, a statute of the United Kingdom Parliament. As Canada gained increasing independence from Britain throughout the nineteenth and early twentieth centuries, an interesting feature of the *British North America Act, 1867* became increasingly irritating: Canada did not have full responsibility for amendment of its own Constitution. As a statute of the United Kingdom, the *British North America Act, 1867*, which effectively was Canada's Constitution, could only be amended by the United Kingdom Parliament.[113]

Following 1867, Canada from time to time requested the United Kingdom Parliament to pass legislation in order to accomplish that which Canadian legal processes could not achieve. Legally speaking, the Westminster Parliament could enact any legislation for Canada whether such legislation was of a constitutional nature or not, and on occasion it did so, dealing with matters as varied as copyrights and lighthouses. Of course, practically speaking, Canada was not as subordinate as this legal relationship indicates. In fact, a convention developed whereby Westminster would legislate only at the request and with the consent of Canada, usually expressed in a Joint Resolution of the Senate and House of Commons.[114]

A small step forward was made with the *Statute of Westminster, 1931*.[115] With regard to the power to amend or patriate the constitution, however, the *Statute of Westminster, 1931* appeared to maintain the *status quo*. In essence, the Statute codified the already accepted convention that Westminster would only pass laws affecting the Dominion if Canada requested the U.K. to do so. The preamble to the *Statute of Westminster* set out the new position of the Dominions in relation to the United Kingdom as recognized by the Balfour Declaration in 1926. The text of the Statute, as already outlined above, did not terminate the ability of the United Kingdom to legislate for the Dominions; instead, it set out the newly restricted terms on which the United Kingdom Parliament could do so. Section 4 of the Statute provided as follows:

> No Act of Parliament of the United Kingdom passed after the commencement of this Act shall extend, or be deemed to extend, to a Dominion as part of the law of that Dominion, unless it is expressly declared in that Act that that Dominion has requested, and consented to, the enactment thereof.[116]

However, the Parliament of the United Kingdom could still, as a matter of law, repeal or disregard section 4 of the Statute. Indeed, the U.K. Parliament could take section 4 to mean that it kept open the legal possibility of legislative action by the U.K. Parliament for Canada, but without Canada's consent.

Given that the *Canada Act, 1982* only went slightly further than the *Statute of Westminster, 1931*, what was there in the patriation process, then, that could be said to irreversibly terminate the legal power of the United Kingdom Parliament over Canada? On Hogg's view, if the United Kingdom did purport to repeal s. 2 of the *Canada Act, 1982*, "it is inconceivable that the Supreme Court of Canada would accept the resuscitated power and uphold the new law".[117] On this view, Canadian courts would decline to recognize the United Kingdom's authority to make law for Canada and the fundamental rule of recognition would shift to Canadian courts.[118] Why is that? On Hogg's view, it is plausible that the fact of independence, and not s. 2 of the *Canada Act, 1982*, is itself sufficient to terminate the United Kingdom's power to enact laws or repeal them for Canada.[119] But, how does the fact of independence answer the objection that the sovereign Parliament of the United Kingdom can legislate for Canada? After all, the Canadian courts had confirmed in 1981 that the power of the United Kingdom to enact constitutional amendments for Canada (prior to 1982) was "unimpaired" and "undiminished".[120]

In other words, under U.K. law, the United Kingdom Parliament can still legislate for Canada just as easily as it can legislate for France, and the British courts will recognize that legislation to the extent possible. As a matter of Canadian law, however, the answer should be that the United Kingdom cannot legislate for Canada. Under the *Canada Act 1982*, the United Kingdom has no power to legislate for Canada after the *Constitution Act 1982* came into force. On Oliver's approach, which we have closely followed here, the patriation of the constitution succeeds not solely from a purported termination of U.K. authority.[121] It succeeds ultimately because of the power and authority that is vested in Canadian lawmakers by the Canadian public as well as the old constitutional roots. As Oliver notes, the patriation succeeds because " . . . those roots and new roots have been and are being put down slowly in popular sovereignty, in regional or provincial vetoes, in aboriginal consents, etc., and a new Canadian constitutional theory will gradually uncover them."[122] Patriation, then, requires a shift in the object of ultimate consent within society. Does this same explanation hold for the patriation of the *.ca* domain?

The Patriation of the *.ca*

The analogy between the politics of the domain space and the politics of real space is striking. One system is the system of legal relations embodied in statutes and common law decisions. The other is a system of norms embodied in computer architecture. In each case, there is a hierarchical system of authority relations. The United Kingdom Parliament and the Courts of the U.K. were superior to the Canadian Parliament, its constitution and Courts. The U.S. controlled root server system is superior to the ccTLDs. In real space, there is a rule of recognition that recognizes the enactments of the U.K.

Parliament as law. In domain space, there is a rule of recognition that recognizes the TLD assignments of the legacy root name server as binding. In each case, there was a delegation of power from a higher level authority. Canadian constitutional powers were delegated by the U.K. Parliament in the enactment of the *British North America Act, 1867*. In the case of CIRA, its powers resulted from a double delegation of power from the Government of Canada and ICANN.

Does the double delegation of power to CIRA entail that Canada is sovereign over the *.ca*? Like the authority of Canada itself, the authority of CIRA is not completely indigenous, derived solely from events occurring within Canada. As was pointed out, the existence of indigenous property law is not sufficient to enable national control over domain mappings and the technical ability to operate the CIRA registry was delegated by a foreign authority, ICANN. Furthermore, under a proposed agreement between CIRA and ICANN, CIRA must adhere to ICANN policies concerning the interoperability of the delegated ccTLD with other parts of the DNS and Internet.[123]

A second explanation of Canada's sovereignty over the *.ca* could be that the U.S. control over the *.ca* has been terminated by mutual recognition of Canada's policy authority over the *.ca*. In fact, ICANN's delegation of power to CIRA, together with ICANN's acknowledgement that Canada has policy authority over the *.ca*, seems to put Canada no further ahead in relation to powers over the *.ca* than it was with the *Statute of Westminster* in the case of constitutional powers. Just as the doctrine of the supremacy of Parliament would not allow the U.K. Parliament to divest itself of authority over Canada, so too the hierarchical nature of the domain name system, with the legacy root server controlled by the U.S. DoC, does not allow authority over domain name assignments to be divested.

Practically speaking, one might claim that Canada can simply ignore any policies that ICANN may want CIRA and its registrants to abide by, just as Taiwan and the world ignore China's attempt to legislate for Taiwan and the U.S. ignores France's Court orders that are unconstitutional under U.S. law.[124] The recognition of U.S. control, however, is embedded in software which is run by every Internet service provider in Canada. These domain name servers recognize the legacy root server, or one of its clones, as authoritative for determining the authoritative ccTLDs. In turn, individual computer users recognize their ISP name servers as authoritative and such recognition is encoded into the computer operating system. Because of the importance of the rules delegating authority to individuals ccTLDs in the root zone file and legacy server and the physical and legal control over the A root zone files and server by the United States government indicates that an entity is authoritative with respect to a country code if and only if it is recognized by the United States government as authoritative.

Therefore, ultimate control over the *.ca* domain will require a change in the technology of the DNS embodying political consent. In the case of the patriation of the Canadian Constitution, the enactment by the United Kingdom of s. 2 of the *Canada Act 1982* together with the shift in consent of the governed accomplished the patriation. Patriation of the *.ca* will, therefore, require not only the recognition of Canada's policy authority by the U.S. and ICANN, but some method of shifting the power and authority of a foreign entity over ccTLDs to that of the Canadian government.

The essence of the patriation of the *.ca* requires that domain name mapping queries should be resolved by national domain registries themselves rather than relying upon a foreign root authority to solve domain name mapping problems. If a URL is typed into a web browser and the DNS server that it queries cannot provide an answer, the DNS server should query a ccTLD authoritative registry server directly rather than ask the root server which registry is authoritative over that domain. Technically, the open-source BIND software which runs most DNS servers would likely have to be modified and/or reconfigured to implement the needed technical changes and new DNS protocols allowing for additional national root servers would need to be created.[125]

Thus, Canada can take it upon itself to "enlarge the root" by creating an additional authoritative root server. Canada could then require domestic ISPs to recognize the national root as authoritative. Essentially, instead of relying on the idea of an authoritative root which is controlled by an independent entity, Canada would retain authority and control over its own domain. The issue that then arises is whether the national root will recognize the legacy root as authoritative.

A second step in the patriation process involves mutual peer-based recognition of authority. This step requires that the national authority no longer recognize the legacy root as an authority. Instead, national roots may directly recognize other national roots as authoritative peers. This peer-to-peer approach can be extended to other name servers as well. Currently, if a local name server cannot provide the answer to a query, such as *gustavmahler.com*, the query is sent to the root which returns the address of the authoritative server for the *.com* domain. On a peer-to-peer account, each name server would point to all the other 243 ccTLD root servers and the 13 Legacy root servers (or indeed, the 14 gTLD registries) as authoritative for their respective domains. Therefore, if someone in Canada looked for *www.google.de*, the resolver would query its local nameserver as to where it should go and, failing a response, then the local name server would direct the query to the German *.de* root server which then resolves the query.[126]

At a political level then, the patriation of the *.ca* would require ccTLDs to recognize each peer country's

ccTLD server as authoritative for such country. Just as patriation required the rewriting of constitutional law, the patriation of the *.ca* will require the rewriting of the constitutional code of the DNS, namely, BIND or other DNS software. Once BIND or other DNS software is modified, reconfigured and implemented as necessary, Internet users will seamlessly use, view, and accept the national authority for each individual ccTLD. Their computers and their queries would be pointed to the relevant country ccTLD server instead of to the previous ultimate sovereign root, indicating a shift in consent to the authoritative country server.

Conclusion

The Government of Canada has purported to delegate authority to CIRA to create and enforce *.ca* policies in accordance with government principles. However, the power of ICANN, backed by the U.S. government, to control the information contained in the legacy root server, ensures that its tacit approval is required for CIRA operations and policy and the use of *.ca* domain names. Claims to sovereignty over ccTLDs based upon property claims are not sustainable and, at any rate, are not sufficient to ensure national control over ccTLDs. Canada does not, therefore, have sovereignty with respect to the *.ca* domain name mappings or policies. Much as Canada required the consent of the U.K. in certain legislative matters prior to the patriation of the Constitution, ICANN's consent is required, at least tacitly, to create and enforce *.ca* policies.

The patriation of the Canadian Constitution was not accomplished solely by delegating law making power to Canada. Nor was the sovereignty of Canada over the *.ca* accomplished by the delegation by ICANN of technical authority to CIRA. Rather, the authority of the Constitution came from a shifting of the focus of consent from the United Kingdom to Canada in the context of a limitation of the power to enact laws for Canada. In analogy with the DNS, it can be said that the courts and people ceased to look to the U.K. courts and Parliament for the ultimate authority and instead began to look to their own courts and Parliament for guidance and rulings. In order to patriate the *.ca* therefore, *.ca* registrants, registrars, ISPs, and other national Internet players must begin to accept the ultimate authority of the Canadian government and its designated entity, CIRA, in relation to the *.ca* domain, rather than that of the ICANN legacy servers. This will require a change in the structure of the DNS itself.

We have recommended that ccTLDs should utilize a non-hierarchical, peer-to-peer ccTLD domain name system based upon the idea that each national domain registry is the final authority over its own ccTLD, derived from the authority of the national government associated with the ccTLD.

Notes:

[1] This association is most reasonable in those countries, such as Canada, where there are "presence requirements" required in order to register a domain name. According to a recent survey by Market Research commissioned by CIRA, 75% of Canadians believe "*.ca*" means Canada; 73% attribute dot-ca Web sites to Canadian organizations and companies; and 90% believe it is important to have the dot-ca domain as a resource for Canadians. See "Canadian Attitudes Toward the Dot-ca Domain" (2001), online: <http://www.cira.ca/official-doc/104.cira_tsc_en.pdf> (accessed June 6, 2002). The claim that country codes in the existing DNS are sovereign has been criticized recently in M. Mueller, *Ruling the Root* (Cambridge: MIT Press, 2002), as a misunderstanding of the function of the legacy DNS. Our claim of sovereignty contained in this paper is with respect to a new DNS that does not possess the same architecture as the legacy DNS.

[2] Online: <http://www.cira.ca> (accessed October 22, 2001).

[3] Online: <http://www.icann.org> (accessed October 22, 2001). IANA, "IANA Report on Request for Redelegation of the *.ca* Top-Level Domain" (2000), online: <http://www.iana.org/reports/ca-report-01dec00.htm> (accessed October 22, 2001) [hereinafter "IANA Report on Request for Redelegation of .ca"].

[4] Letter from Michael Binder, Industry Canada, to Robert Hall dated March 11, 1999, CIRA, online: <http://www.iana.org/reports/industry-canada-letter-11mar99.htm> (accessed October 22, 2001).

[5] Industry Canada notes that a "crucial reason for an independent country code top level domain policy involves the work under way in Canada on the .ca domain and its potential importance for Canadian Internet users," Industry Canada, "Domain Name System Reform and Related Internet Governance Issues: A Consultation Paper" (1998), online: <http://e-com.ic.gc.ca/english/strat/651d1.html> (accessed October 22, 2001) [hereinafter "Domain Name System Reform"].

[6] M. Froomkin, "Wrong Turn in Cyberspace: Using ICANN to Route around the APA and the Constitution" (2000), online: <http://www.law.tm>; J. Weinberg, "ICANN and the Problem of Legitimacy" (2000) 50 Duke L.J. 187, online: <http://www.law.duke.edu/shell/cite.pl?50+Duke+L.+J.+187> (accessed October 22, 2001).

[7] *Ibid.*

[8] M. Froomkin and M. Lemly, "ICANN and Antitrust" (2002), online: <http://www.law.tm> (Draft Manuscript) (accessed October 22, 2001).

[9] M. Geist, "Fair.com: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP" (2001), online: <http://aix1.uottawa.ca/~geist/> (accessed October 22, 2001).

[10] L. Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 2000).

[11] This paper does not explore these legal and implications in detail. Instead it explores the analogy between the patriation of the Canadian Constitution and the proposed patriation of the *.ca* domain. For further discussion on these policy implications see K. G. von Arx and G. R. Hagen, "Sovereign Domains", forthcoming in the Richmond Journal of Law and Technology, G. R. Hagen, "Sovereign Domains and Property Claims" (forthcoming), and K. G. von Arx, "ICANN — Now and Then: ICANN's Reform and Its Problems" (forthcoming).

[12] ICANN. ICP-3, "A Unique Authoritative Root for the DNS" (2001), online: <http://www.icann.org/icp/icp-3.htm> (accessed October 22, 2001).

[13] *Ibid.* ICANN has established an internal policy that, for technical reasons, there must be "unique authoritative root for the domain name system".

[14] S. Brand, "Founding Father" (2001), online: <http://www.wired.com/wired/archive/9.03/baran.html?pg=1&topic=&topic_set> (accessed October 22, 2001).

[15] D. Reed, "End-to-End Argument in System Design", online: <http://www.reed.com/Papers/EndtoEnd.html> (accessed October 22, 2001).

[16] D. Isenberg, "Rise of the Stupid Network", online: <http://www.rageboy.com/stupidnet.html> (accessed October 22, 2001).

[17] P. Albitz and C. Liu, *DNS and BIND*, 3rd ed. (New York: O'Reilly, 1998), chapter 2 online: <http://www.oreilly.com/catalog/dns3/chapter/ch02.html> (accessed July 12, 2002).

[18] For a complete list of the current 14 gTLDs and the requirements for obtaining some of them, see "Generic Top Level Domains", online: <www.iana.org/gtld/gtld.htm> (accessed February 23, 2002).

[19] However, note that *.mil* (for military) and *.gov* (for government) are reserved for U.S. use only and *.edu* is reserved for educational organizations accredited one of the six U.S. regional accrediting agencies.

[20] See "Infrastructure Top Level Domain", online: <www.iana.org/arpa-dom/> (accessed July 12, 2002).

[21] Names in the newer gTLDs are allocated in more complex fashions that give priority to trademark holders, and also seek to level the playing field for similarly situated applicants competing for a name during the initial rush period when registrations open.

[22] Note there are 13 root servers which are assigned letters from A–M. The U.S. operates the "E", "G", and "H" root servers. The U.S. contracted out operations of the "A", "B", and "L" root servers. "C" and "D" are operated by non-governmental, U.S.-based entities. And only the "I", "K", and "M" root servers are operated in other countries. See D. Conrad, A. Kato and B. Manning, "Root Nameserver Year 2000 Status" (1999), online: <http://www.icann.org/committees/dns-root/y2k-statement.htm> (accessed October 22, 2001). Like the notion of the Internet itself, the notion of a unique legacy root zone file is a logical notion and not physical. In reality, only the A root server is authoritative and the mappings of the A root file are copied to the other 12 physically distinct secondary root server "clones".

[23] Albitz and Liu, *supra* note 17.

[24] Of course, it is possible to define a unique set of mappings in an alternative DNS, which may even include the legacy DNS as a part. It is simply a mathematical truth that there exists multiple families of unique mappings from domain names to IP addresses.

[25] "A Unique Authoritative Root for the DNS", *supra* note 12.

[26] For other examples of centres of control on the Internet, see M. Blumenthal and D. Clark, "Rethinking the design of the Internet: The end to end arguments vs. the brave new world" (2001), online: <http://ana.lcs.mit.edu/anaweb/PDF/Rethinking_2001.pdf> (accessed October 22, 2001) and D. Reed, "The End of the End to End Argument?," online: <http://www.reed.com> (accessed October 22, 2001).

[27] Reed, *ibid.*

[28] United States Department of Commerce, "Improvement of Technical Management of Internet Names and Addresses; Proposed Rule" (1998) online:<http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.htm> (accessed October 22, 2001).

[29] United States Department of Commerce, "Management of Internet Names and Addresses" (1998), online: <http://www.icann.org/general/white-paper-05jun98.htm> (accessed October 22, 2001).

[30] Mueller, *supra* note 1 at chapter 8.

[31] *Supra* note 29 at para. 11.

[32] *Ibid.*

[33] *Ibid.*

[34] *Ibid.*

[35] Industry Canada, "Reform of the Domain Name System: Current Developments & Statement of Principles: An Information Paper Prepared by Industry Canada with the assistance of Omnia Communications Inc." (1998), online: <http://e-com.ic.gc.ca/english/strat/651d2.html> (accessed October 22, 2001).

[36] Nor has it become accountable and transparent. See Froomkin, *supra* note 6 and Weinberg, *supra* note 6.

[37] General Accounting Office, "Letter to Subcommittee on Commerce, Justice, State, and the Judiciary dated July 7, 2000," online: <http://www.icann.org/general/gao-report-07jul00.pdf> (accessed October 22, 2001).

[38] *Ibid.*

[39] Quoted in S. Kettmann, "Will US Release Grip on ICANN?" Wired News, January 19, 2002, online: <http://www.wired.com/news/infostructure/0,1377,49836,00.html> (accessed March 29, 2002).

[40] Letter from Energy and Commerce Committee to Secretary Donald L. Evans dated March 13, 2002, online: <http://www.politechbot.com/p-03268.html> (accessed March 31, 2002).

[41] Quoted in Kettman, *supra* note 39.

[42] Memorandum of Understanding Between U.S. Department of Commerce and ICANN, online: <http://www.icann.org/general/icann-mou-25nov98.htm> (accessed October 22, 2001).

[43] *Ibid.*

[44] *Ibid.* at Article VII.

[45] No agreement has been made between ICANN and CIRA as of this date. However, see the termination provisions under the *.au* and *.jp* Sponsorship Agreements, online: <http://www.icann.org/cctlds/au/sponsorship-agmt-25oct01.htm> and <www.icann.org/cctlds/jp/sponsorship-agmt-27feb02.htm> respectively (accessed March 26, 2002).

[46] S. Lynn, "ICANN — The Case for Reform" (2000), online: <http://www.icann.org/general/lynn-reform-proposal-24feb02.htm> (accessed February 28, 2002)

[47] ICANN. "Model ICANN-ccTLD Manager Memorandum of Understanding — Legacy Situation", online: <http://www.icann.org/cctlds/model-legacy-mou-23mar02.htm> (accessed July 28, 2002).

[48] See Mueller, *supra* note 1 at 212.

[49] ICANN. "Model Sponsorship Agreement, Triangular Situation", online: <http://www.icann.org/cctlds/model-tscsa-31jan02.htm> (accessed August 28, 2002) [hereinafter "Model Sponsorship Agreement, Triangular"].

[50] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, Schedule I, s. 4.5.

[51] *Ibid.*

[52] *Supra* note 2.

[53] "Management of Internet Names and Addresses", *supra* note 29.

[54] "Domain Name System Reform", *supra* note 5.

[55] Perhaps this could be inferred from the Letter from Michael Binder, Industry Canada, to Michael Roberts dated October 10, 2000, ICANN, online: <http://www.iana.org/reports/industry-canada-letter-10oct00.htm> (accessed October 22, 2001). Additional evidence is from the membership of GOC in GAC.

[56] Letter from Binder to Hall, *supra* note 4.

[57] *Supra* note 2.

[58] Letter from Binder to Hall, *supra* note 4.

[59] Governmental Advisory Committee (GAC), "ICANN Governmental Advisory Committee Operating Principles," online: <http://www.noie.gov.au/projects/international/DNS/gac/docs/Operating_Principles-English.htm> (accessed October 22, 2001) [hereinafter "GAC Operating Principles"]. Canada is a member of GAC. Membership in the GAC is open to national governments, distinct economies as recognised in international fora, multinational governmental organizations and treaty organizations, and public authorities, each of which may appoint one representative to the GAC. The GAC provides advice on the activities of ICANN as they relate to concerns of members, and distinct economies as recognised in international fora, including matters where there may be an interaction between ICANN's policies and various laws and international agreements and public policy objectives.

[60] Letter from Binder to Hall, *supra* note 4.

[61] IANA was the predecessor organization that was mandated by the U.S. government to manage the TLD space for the entire Internet.

[62] Canadian Domain Name Consultative Committee, "Framework for the Administration of the Canadian Internet Domain Name .Ca" (1998), online: <http//www.cira.ca/official-doc/12.CDNCC_Final_Report.doc> (accessed October 22, 2001).

[63] *Ibid.*

[64] *Ibid.*

[65] The CDNCC was composed of representatives from the .ca Committee of the Canadian Internet Society, Canadian Association of Internet service Providers and the Federal Government.

[66] "Reform of the Domain Name System", *supra* note 35.

[67] Letter from Binder to Roberts, *supra* note 55.

[68] *Ibid.*

[69] "IANA Report on Request for Redelegation of .ca", *supra* note 3.

[70] The amicability of the transfer was no doubt enhanced by the fact that the University of British Columbia was paid nearly $4.5 million dollars

for compensation for its role in developing the *.ca* domain. See "Transition Agreement for the Transfer of the .ca domain name registry," online: <http://www.cira.ca /official-doc/32.Transitition_agreement.pdf> (accessed October 22, 2001).

[71] IETF, "RFC 1591: Domain Name System Structure and Delegation," online: <http://www.isi.edu/in-notes/rfc1591.txt> (accessed October 22, 2001).

[72] ICP-1, online: <http://www.icann.org/icp/icp-1.htm> (accessed March 28, 2002).

[73] Under RFC 1591, prior to any transfer of the designated manager trusteeship from one organization to another, the higher-level domain manager (the IANA in the case of top-level domains) must receive communications from both the old organization and the new organization that assures ICANN that the transfer in mutually agreed, and that the new organization understands its responsibilities. Thus, letters were exchanged by the parties memorializing the transfer of authority.

[74] Letter from Binder to Hall, *supra* note 4.

[75] For an account, see J. Malcolm, "Who controls .Org.au? Where domain policy and law collide", online: <http://dnsaction.terminus.net.au/dnsarticle.pdf> (accessed October 22, 2001); IANA, "IANA Report on Request for Redelegation of the .au Top-Level Domain" (2001), online: <http://www.iana.org/reports/au-report-31aug01.htm> (accessed October 22, 2001) [hereinafter "IANA Report on Request for Redelegation of .au"].

[76] Australia signed the ccTLD Sponsorship Agreement (.au) on October 25, 2001. See online: <http://www.icann.org/cctlds/au/sponsorship-agmt-25oct01.htm> (accessed March 26, 2002).

[77] *Supra* note 73.

[78] Robert Elz, who was the original delegate of authority to administer the *.au* name space created a number of second level domains and delegated a number of second level domains to independent domain name registrars according to policies of his devising, and all of which was consistent with then current IANA policies. Elz retained the registration functions for *.org.au* and *.id.au*. Both second level domains were redelegatged from Elz to *.au* Domain Administration, the auDA registry.

[79] ICP-1, *supra* note 72.

[80] "IANA Report on Request for Redelegation of .au", *supra* note 75.

[81] *Ibid.*

[82] "GAC Operating Principles", *supra* note 59.

[83] See for example, the Letter from Newman & Newman Attorneys at Law, LLP to Vice President of IANA, Louise Touton, dated December 13, 2001 regarding the *.cx* (Christmans Islands), online: <http://www.wwtld.org/Tracking_IANA/CX_Touton_Nameserver_Changes_20011213.pdf> (accessed March 28, 2002). To this date, there still has not been a redelegation of *.cx*.

[84] ICANN Announcement, "Redelegation of .us Country-Code Top-Level Domain", (2001), online: <http://www.icann.org/announcements/announcement-19nov01.htm> (accessed March 28, 2002). Apparently a full report will be posted "as soon as it is complete". None has been issued yet.

[85] *Ibid.*

[86] *Ibid.*

[87] GAC, "Executive Minutes" from Los Angeles Meeting on November 2, 1999, online: <http://www.noie.gov.au/projects/international/DNS/gac/meetings/mtg4/gac4min.htm> (accessed August 28, 2002); GAC, "Scribe's Notes" from Cairo Meeting on March 8, 2000, online: <http://cyber.law.harvard.edu/icann/cairo/archive/scribe-gac-030800.html> (accessed August 28, 2002).

[88] "GAC Operating Principles", *supra* note 59.

[89] G. Calabresi and A.D. Malamed, "Property Rules, Liability Rules and Inalienability: One View from the Cathedral" (1972) 85 Harv. L. Rev. 1089.

[90] See the discussion in Malcolm, *supra* note 75.

[91] *Ibid.*

[92] Quoted in Malcolm, *ibid.* See also *Network Solutions, Inc. v. Umbro International Inc.*, 529 S.E.2d 80, [2000] W.L. 117760 (Va. 2000).

[93] 194 F.3d (9th Cir., 2000).

[94] 99 F.Supp.2d 1168, [2000] W.L. 1811403 (N.D.Cal., 2000).

[95] 15 U.S.C. § 1125(d). See, for example, *Porsche Cars North America v. Porsche.com*, 51 F.Supp.2d 707 vac. and remanded 215 F.3d 1320 (E.D.Va. 1999), online: <http://laws.lp.findlaw.com/4th/012028p.html>.

[96] Malcolm, *supra* note 75.

[97] *Caesar's World Inc. v. Caesars-Palace.com*, 112 F.Supp.2d 502 (E.D. Va. 2000).

[98] For a discussion that argues in favour of domain names being the subject of property rights, see X. Nguyen, "Cyberproperty and Judicial Dissonance: The Trouble With Domain Name Classification" (2001) 10 Geo. Mason L. Rev. 183.

[99] (2001) 14 C.P.R. (4th) 22, 202 D.L.R. (4th) 560 (Ont. Sup. Ct.) [hereinafter *Easthaven*].

[100] *Ibid.*

[101] *Ibid.*

[102] J.P. Barlow, "A Cyberspace Independence Declaration," online: <http://www.eff.org/Publications/John_Perry_Barlow/barlow_0296.declaration> (accessed October 22, 2001).

[103] D. Johnson and D. Post, "Law And Borders — The Rise of Law in Cyberspace" (1996) 48 Stan. L. Rev. 1367. See also Easthaven, *supra* note 99 at 570 (D.L.R.). As Whitten J. observed in *Pro-C Ltd. v. Computer City Inc.* (2000), 7 C.P.R. (4th) 193 at para. 1: "The Internet, in reality a network of networks, has created a whole new territory independent of conventional geography."

[104] D. Post. "Cyberspace's Constitutional Moment" (1998), online: <http://www.temple.edu/lawschool/dpost/DNSGovernance.htm> (accessed July 12, 2002).

[105] D. Post, "The 'Unsettled Paradox': The Internet, the State, and the Consent of the Governed" (1998) 5 Indiana J. Global Leg. Stud. 521.

[106] *Ibid.*

[107] P.W. Hogg, *Constitutional Law of Canada* loose-leaf (Toronto: Carswell 1997) Vol. 1 at s. 3.5(a).

[108] *Ibid.* at s. 3.5(c). In contrast, the constitution of the United States is autochthonous since, after the American revolution, which broke the chain of authority from the U.K., authority sprang from within the U.S.

[109] *Ibid.*

[110] *Canada Act 1982*, (U.K.) 1982, c. 11.

[111] This is the mysterious doctrine of the divisibility of the Crown. It is a curious fact that the sovereignty of Canada still rests with the Queen of Canada, but not the Queen of the United Kingdom.

[112] See Peter Oliver's discussion of Alf Ross's view, in P. Oliver, "The 1982 Patriation of the Canadian Constitution: Reflections on Continuity and Change'' (1994) 28 Thémis 877 , online: <http://www.lexum.umontreal.ca/themis/94vol28n2-3/OLIVER.html> (accessed October 22, 2001).

[113] *Reference re Amendment of the Constitution of Canada*, [1981] 1 S.C.R. 753 [hereinafter "Patriation Reference"].

[114] Oliver, *supra* note 112.

[115] 22 Geo. 5, ch. 4 (U.K.).

[116] *Ibid.*

[117] Hogg, *supra* note 107 at s. 3.5(d).

[118] Oliver, *supra* note 112.

[119] Hogg, *supra* note 107 at s. 3.5(d).

[120] "Patriation Reference", *supra* note 113.

[121] Oliver, *supra* note 112.

[122] *Ibid.*

[123] "Model Sponsorship Agreement, Triangular", *supra* note 49.

[124] *The French Union of Jewish Students and The League Against Racism and Anti-Semitism v. Yahoo! Inc.*, *The County Court of Paris* (Orders of May 22 and Nov. 20, 2000) and *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F.Supp.2d 1181 (2001).

[125] This solution requires the adoption of a system of alternative roots. While this approach has been extensively criticized by ICANN, its own protocol supporting organization has admitted that it is possible to devise such a system of multiple roots. Minutes, ICANN Protocol Standards Organization, September 4, 2001, (emphasis added), online: <http://www.pso.icann.org/PSO_Minutes/PSO-Minutes-4Sept2001.txt>. This statement was reconsidered and reconfirmed at the September 28, 2001, meeting, online: <http://www.pso.icann.org/PSO_Minutes/PSO-Minutes-28Sept2001.txt> (accessed October 22, 2001).

[126] Apparently, major ISPs already cache the addresses of the TLD registries in order to avoid accessing the root as often as without such caching. See

Mueller, *supra* note 1 at 50. The present proposal extends this system to national roots as well. Unfortunately, however, present technical limitations limit the root to 13 servers. While this system is not peer-to-peer at a level of individual users, it is peer-to-peer at the level of ccTLDs.